Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 47 (2015) 480 – 485

Procedia Computer Science

Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud

Sujithra M[a], Padmavathi G [b], Sathya Narayanan[c]

[a,c]*Department of Computer Technology & Applications, Coimbatore Institute of Technology, Coimbatore, TN, India* [b]*Department of Computer Science, Avinashilingam Institute of Home Science and Higher Education for Women, Coimbatore, TN, India*

Abstract

In the technology up-front world, mobile devices like smartphones and tablets are inevitable. When computing capacity and storage need of these devices are increasing tremendously, it demands the secure way of storing the data in cost efficient model. This paper describes how securely the mobile data can be stored in the remote cloud using cryptographic techniques with minimal performance degradation

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)

Keywords: Mobile Data security; Cryptographic techniques; Performance metrics

1. Introduction

Increase in mobile device sophistication also demands high storage sophistication. Mobile Cloud Computing (MCC) service, allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs. Also, increase in feature rich mobile applications like mobile wallets, banking apps, and healthcare app etc. exposes sensitive data of the users which are always prone to much vulnerability. The value of data is far more important than the value of device. The main issue in using MCC is securing the user data on mobile cloud since there is a high risk of unauthorized access to the data. So the main concern of cloud service provider is to provide data security by the same time providing ease of access to the authorised user. New service architectures are necessary to address the security concerns of the mobile data, without any performance issue. Considering all these constraints a research has been performed and this paper briefs its result.

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)
doi:10.1016/j.procs.2015.03.232

Smart phones have certain security mechanism in place to deal with unauthorized access to sensitive and secret data. The most common protection mechanism is password based protection [2]. User assign password to critical files and data. This password is then used to allow access or deny based upon the correct or incorrect password. This approach has some drawback. The major one is that the password can be seen by others. The unauthorized user attacker can then later use the same password to get an entry into secured data. Pattern used for providing security also have the same problems. Biometric based security is also in place but requires precision and cannot be shared with others in case of emergency. The more advanced security approach is to encrypt the data by the strong encryption algorithm.

2. Cryptographic Approach

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. We propose a suitable method that cryptographic algorithms with different key lengths are used in various environments. The number of mobile devices such as smart phones and smart pads grows rapidly recently. End users can access easily to cloud computing environment thought these mobile devices we define that mobile cloud computing is one of specific services of cloud computing and it is a mobile service which is added a cloud computing service.

According to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem, asymmetric cryptosystem and digital signature. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), AES (Advanced Encryption Standard). For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret. The representatives of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem). For Digital signature the representatives is MD5 and SHA1.

3. Proposed Work

The encrypted data is stored in smart phone memory which is then later used for accessing by decrypting the data. All of these method usually processes and computes in the memory of smart phone which is still prone to unauthorized access. In case of lost or theft of smart phone the unauthorized person can have access to the device and a technically proficient person can get an entry into data as encryption techniques are all present on the device itself [2]. In order to overcome these problems, three-tier security using cloud architecture is being proposed as a hybrid approach. In three-tier hybrid approach, as a First tier security, encryption is done using MD5 algorithm with the key (k1) given by the user. As Second-tier security, these encrypted data are again encrypted using AES algorithm. As a third-tier security further encryption of data or key using ECC or RSA algorithm is performed respectively, ensuring more security and the key is shared with the user. All the above methods are performed in both Local and remote environment as shown in the below figure 1.

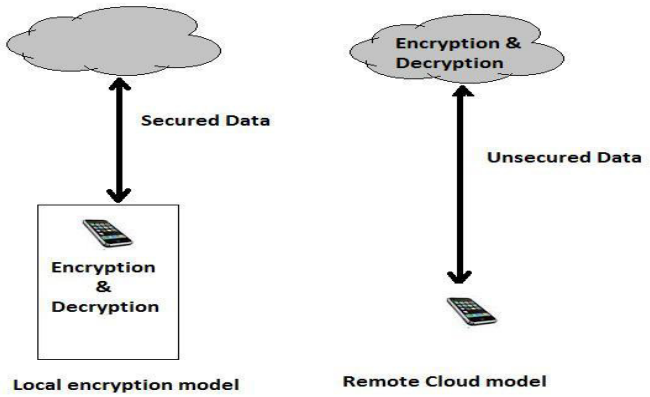

Fig: 1 Practiced Encryption Models

3.1 Implemented Algorithms

The cryptographic algorithms used are Symmetric key algorithms, Asymmetric key algorithms and Combination of these algorithm as a Hybrid Approach. Evaluation metrics for these algorithms are studied based on various previous research work. Encryption techniques will make the data more secure in the local system as well as on the remote cloud. Test has been executed in both the above environment using the following algorithms one at a time.

- AES: In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
- DES: The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm in the world. For many years, and among many people, "secret code is making" and DES have been synonymous meaning it operates on plaintext blocks of a given size (64-bits) and returns cipher text blocks of the same size.
- RSA: RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It protected user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission
- MD5: a widely used cryptographic hash function with a 128-bit hash value processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.
- Elliptic Curve Cryptography (ECC) with SHA-512: An elliptic curve is given by an equation in the form of The finite fields those are commonly used over primes (FP) and binary field (F2n). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDCP). This problem is defined as: Given point X, Y on elliptic curve, find z such that X=zY. The following steps describe how ECC works with SHA-512 [9], [10]. ECC key generation: To generate a public and private key pair for use in ECC communication the steps followed are:

  Find an elliptic curve E(K), where K is a finite field such as Fp or F2n, and a find point Q on E(K). n is the order of Q.

  Select a pseudo random number x such that $1 \leq x \leq (n - 1)$. Compute point $P = xQ$.

  ECC key pair is (P, x), where P is public key, and x is private key.
- MD5, AES, ECC Hybrid approach: In order to increase the level of security, hybrid of Symmetric and asymmetric key algorithms are used. In this method, actual data is encrypted with MD5 algorithm and the encrypted file is further encrypted with AES and then with ECC ensuring 3 levels of encryption.
- MD5, AES&RSA Hybrid approach: In this technique, actual data is encrypted with MD5 and the encrypted file is further encrypted using AES algorithm. Unlike the previous method, here the generated AES key is encrypted using RSA rather than encrypting the actual data.

Cloud architecture is designed by combining cryptographic algorithms with Mobile device environment. The cryptographic algorithms to be used are selected based on comparative study from previous researches. So the symmetric, asymmetric and digital signature algorithms AES, DES, RSA, ECC, and MD5 are selected and used for cryptographic application. The cryptographic application is used to encrypt and decrypt data, provides options to application user whether to use asymmetric with digital signature or symmetric algorithm.

Steps Performed:

- Create some input data samples of sizes 25kb, 50kb, 75kb, 100kb, 125kb and 150 kb.
- Run the cryptographic algorithms with all input data sizes in mobile device.
- Make a cloud server instance on application tool and then make a dynamic web project.
- Run the encryption algorithms on cloud server input data sizes and note all observations
- Compare both the results.

Results are compared based on the performance metrics Mean Processing Time and Speed-Up Ratio.

Mean Processing Time:

Mean processing time is the difference between the starting time taken to encrypt the data and the ending time. It is also evaluated both on single system and on cloud network. It is the difference between the time taken to encrypt the data. As the size of input increases the time taken to encrypt the data will increase and with the increase in time speed-up ratio decreases.

Speed-Up Ratio:

It is defined as the difference between the mean processing time of single system and the cloud network. Speed-up ratio will provide tell us how fast the data have been encrypted. It will give us the idea about speed of encryption.

Speedup Ratio = Processing Time in Local − Processing Time in Cloud

4. Results Observed

Figure 2, 3, 4, 5, 6 are the results observed while performing the above analysis.

CLOUD

	Encryption							Decryption						
Size	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES
25	0.003	0.012	0.043	0.018	68.082	18.736	0.046	0.004	0.020	3.603	0.019	8.192	11.425	3.520
50	0.004	0.015	0.066	0.008	149.105	36.818	0.106	0.006	0.032	3.550	0.008	86.697	22.529	3.601
75	0.005	0.022	0.035	0.028	250.780	55.098	0.132	0.015	0.032	3.547	0.012	145.986	53.528	3.569
100	0.015	0.030	0.048	0.021	330.595	73.243	0.134	0.011	0.030	3.579	0.014	200.769	45.133	3.582
125	0.023	0.038	0.030	0.015	522.671	232.564	0.150	0.012	0.039	3.600	0.025	281.478	294.979	5.287
150	0.012	0.044	0.037	0.017	636.106	286.087	0.123	0.021	0.044	3.571	0.026	263.552	423.975	3.609

Local

	Encryption							Decryption						
Size	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES
25	0.345	0.012	0.109	0.075	740.011	63.704	0.113	0.145	0.020	6.615	0.152	369.992	50.963	7.263
50	0.326	0.015	0.174	0.130	1045.055	161.999	0.101	0.136	0.032	7.355	0.281	522.503	147.419	7.050
75	0.454	0.022	0.100	0.167	1456.445	198.352	0.492	0.203	0.032	7.701	0.427	560.147	184.467	6.353
100	0.632	0.030	0.089	0.231	1668.667	322.271	0.098	0.207	0.030	8.237	0.609	667.449	302.934	6.720
125	0.796	0.038	0.078	0.269	2013.605	790.719	0.196	0.251	0.039	4.847	0.758	805.419	735.368	5.018
150	0.921	0.044	0.324	0.359	2301.879	1058.522	0.212	0.295	0.044	6.383	0.852	885.311	973.840	4.755

Fig: 2 Mean-Processing time table

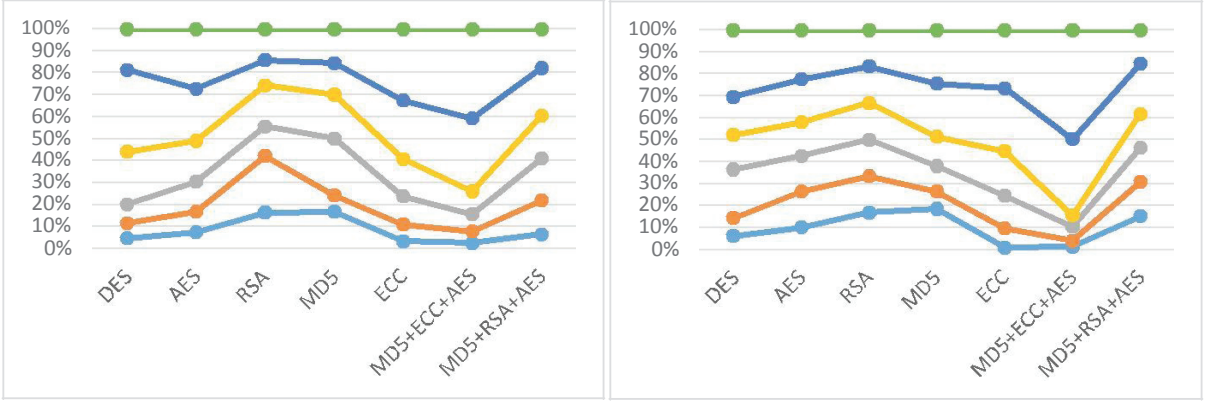

Fig: 3 Encryption and Decryption in Cloud Environment

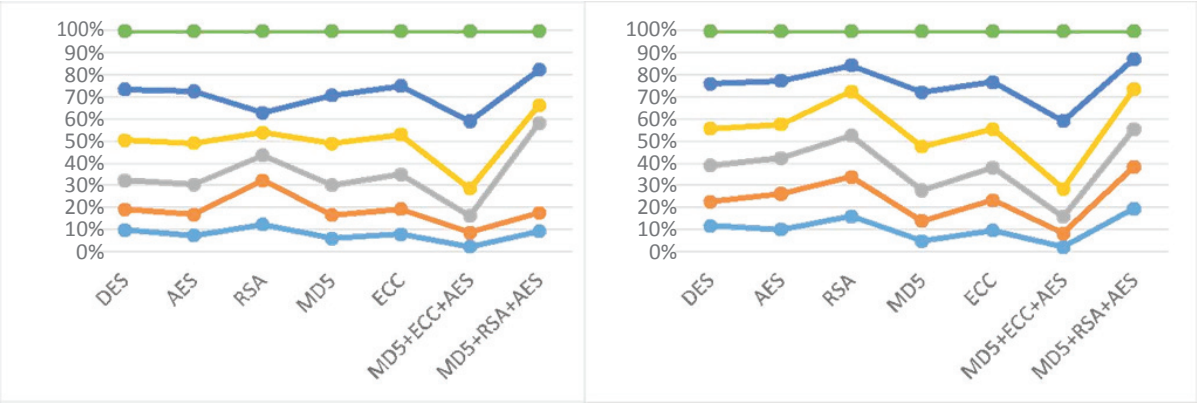

Fig: 4 Encryption and Decryption in Local Environment

Speed_up_ratio														
	Encryption							Decryption						
Size	DES	AES	RSA	MD5	ECC	MD5+ECC+AES	MD5+RSA+AES	DES	AES	RSA	MD5	ECC	MD5+ECC+	MD5+RSA+AES
25	0.342000	0.000000	0.066667	0.057333	671.929333	44.967200	0.067000	0.141000	0.000000	3.011667	0.132667	361.799333	39.537827	3.743000
50	0.321333	0.000000	0.108000	0.122333	895.950000	125.181200	-0.004667	0.130333	0.000000	3.805333	0.272333	435.806333	124.890605	3.449667
75	0.448667	0.000000	0.065333	0.139333	1205.664667	143.253933	0.360000	0.187333	0.000000	4.153667	0.415000	414.161821	130.938655	2.784000
100	0.617000	0.000000	0.041667	0.209667	1338.071667	249.027333	-0.035667	0.195667	0.000000	4.658000	0.594667	466.679667	257.801427	3.138333
125	0.772667	0.000000	0.048333	0.253333	1490.934000	558.154400	0.046000	0.239000	0.000000	1.246667	0.733000	523.940333	440.389755	-0.268667
150	0.909000	0.000000	0.287667	0.342000	1665.773667	772.434900	0.088667	0.273667	0.000000	2.812333	0.826667	621.758462	549.865481	1.145333

Fig: 5 Speed-Up ratio table

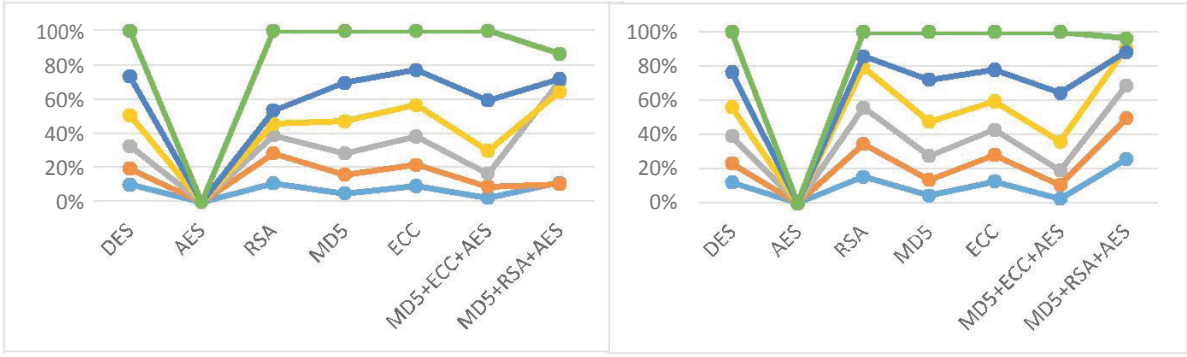

Fig: 6 Speed-up Ratio Chat for Encryption and Decryption

5. Conclusion and Future Work

In the older techniques these cryptographic algorithms are implemented in the Single system environment. Now due to availability of high performance computing techniques, similar test has been conducted in the single system environment i.e. local environment and also in the Cloud environment. From the observed results, and based on the considered parameters, storing the mobile data in cloud increases the efficiency. Also the results reveal that AES algorithm qualifies better than other algorithms in Mean processing time and combination of MD5+ECC+AES algorithm qualifies better than others in Speed-Up ratio. Since it is not wise to take a decision

considering only these parameters, other performance measures like Turn-around time, Throughput are planned to be included in the future work.

References

1. Kumar, K., Lu, Y.-H.: Yung-Hsiang Lu: Cloud Computing for Mobile Users: Can Offloading Computation Save Energy? Computer 43(4), 51– 56 (2010)
2. Simoens, P., De Turck, F., Dhoedt, B., Demeester, P.: Remote Display Solutions for Mobile Cloud Computing. Computer 44(8), 46–53 (2011)
3. Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review," Journal of Emerging Trends in Computing and Information Sciences, 2012.
4. Shashi Mehrotra Seth, Rajan Mishra, “Comparative Analysis Of Encryption Algorithms For Data Communication," IJCST Vol. 2, Iss ue 2, June 20 I I .
5. Shahryar Shafique Qureshi1 , Toufeeq Ahmad1, Khalid Rafique2, Shuja-ul-islam3 “Mobile cloud computing as future for mobile applications – implementation methods and challenging issues”-2011.
6. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD
7. 29. Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18
8. Pearson, S., Y. Shen, and M. Mowbray, “A Privacy Manager for Cloud Computing”, in Proceedings of the 1st International Conference on Cloud Computing. 2009, Springer-Verlag: Beijing, China. p. 90-106.
9. Wang, Q., et al., “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”, in Computer Security – ESORICS 2009, M. Backes and P. Ning, Editors. 2009, Springer Berlin / Heidelberg. p. 355-370.
10. Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. A Survey of Mobile Cloud Computing: Architecture Applications, and Approaches,In Wireless Communications and Mobile Computing 2011.
11. Wei Ren, Linchen Yu, Ren Gao, Feng Xiong.Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing. Tsinghua Science And Technology,ISSNl1007-0214ll06/09llpp520 528.Volume 16, Number 5, October 2011.
12. Liu Q, Wang G, Wu J. Efficient sharing of secure cloud storage services. In: 2010 IEEE 10th International Conference on Computer and Information Technology (CIT10). Bradford, West Yorkshire, UK, 2010: 922-929.
13. Jim Luo And Myong Kang, 2011.“Application Lockbox for mobile device security” Aman Sagar, Sanjeev Kumar, Palladium in Cryptography: The Advancement in Data Security, HCTL Open International Journal of Technology Innovations and Research, Volume 7, January 2014, ISSN: 2321-1814, ISBN: 978-1-62951-250-1.
14. P. Syam Kumar, R. Subramanian and D. Thamizh Selvam, Ensuring Data Storage Security in Cloud Computing using Sobol Sequence, 978-1-4244- 7674-9/10., IEEE, 2010.
15. Rahul Bhatnagar, Suyash Raizada, Pramod Saxena, SECURITY IN CLOUD COMPUTING ,International Journal For Technological Research In Engineering, ISSN (Online) : 2347 4718, December - 2013.
16. Venkata Sravan Kumar, Maddineni Shivashanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master Thesis Electrical Engineering, School of Computing Blekinge Institute of Technology SE – 371 79 Karlskrona Sweden, November 2011.
17. K. Kumar and Y. H. Lu, “Cloud Computing For Mobile Users: Can Offloading Computation Save Energy?,” IEEE Journal Computer, vol.43, pp. 51-56, April 2010.
18. E. Lagerspetz and S. Tarkoma, “Mobile Search and the Cloud: The Benefits of Offloading,” IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 117–122, March 2011.
19. X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham , and S. Jeong, “Securing Elastic Applications on Mobile Devices for Cloud Computing,” Proc. ACM Workshop on Cloud Computing Security (CCSW '09), pp. 127-134, November 2009
20. W. Ren, L. Yu, R. Gao, and F. Xiong, “Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing,” Journal of Tsinghua Science and Technology, vol. 16, pp.520-528, October 2011.
21. W. Itani, A. Kayssi, and A. Chehab, “Energy-efficient Incremental Integrity for Securing Storage in Mobile Cloud Computing,” Proc. Int. Conference on Energy Aware Computing (ICEAC '10), pp. 1-2, December 2010.
22. S.C. Hsueh, J.Y. Lin, and M.Y. Lin, “Secure Cloud Storage for Conventional Data Archive of Smart Phones,” Proc. 15th IEEE Int. Symposium on Consumer Electronics (ISCE '11), pp. 156-161, June 2011.
23. J. Yang, H. Wang, J. Wang, C. Tan, and D. Yu1, “Provable Data Possession of Resource Constrained Mobile Devices in Cloud Computing,” Journal of Networks, vol. 6, pp. 1033-1040, July 2011.
24. Z. Zhou and D. Huang, “Efficient and Secure Data Storage Operations for Mobile Cloud Computing,” IACR Cryptology ePrint Archive, 2011.
25. D. S. Abdul.Elminaam, H. M. Abdul kader, M. M. Hadhoud. " Evaluating the Effects of Cryptography Algorithms on Power Consumption for Different Data Types ".International Journal of Network Security (IJNS),VOL.11 No.2, pp: 91- 100, Sep 2010.